Time synchronization for the Gauntlet Firewall

Here is some information about switching the time synchronization for the AWIPS Gauntlet firewalls from AS1/AS2 to DX1/DX2. **********

After the DX/NAS was installed, the time server for the Network Time Protocol (NTP) moved from the AS1/AS2 servers to the DX1/DX2 servers. The following procedure describes how to configure the AWIPS Gauntlet firewall system to receive the NTP time broadcasts from the DX1/DX2 servers so that the time on the AWIPS Gauntlet firewall system is correctly set.

Configurations for the Network Time Protocol on the Gauntlet Firewall server, the gw server

1. At an AWIPS workstation, open a telnet window and log into the **ds1** server as the root user. Enter the following commands:

   ```
   cd  /etc
   grep  dx1-lll  hosts          where lll is the AWIPS identifier for your office
   grep  dx2-lll  hosts
   grep  ls1-lll  hosts
   ```

   The IP addresses for these servers are utilized in the following steps so please write this information in the space provided:

   dx1   ____.____.____.____

   dx2   ____.____.____.____

   ls1   ____.____.____.____

2. The procedure outlined in this step provides a method for logging into the Gauntlet Firewall server from the ds1 server. This is the procedure which is utilized by the SST/NCF technical support to log into the Gauntlet firewall. However, if you are more familiar with the login from the System Console to the Gauntlet Firewall server, you can perform the System Console login procedure in order to prepare you for step 3.

   a. From the telnet window which is logged into **ds1**, log into the Gauntlet Firewall by entering the following commands:

   ```
   export  TERM=vt100
   telnet  xyplex1  2000
   ```

   After the telnet xyplex1 2000 command, the following connection message will be displayed from the AWIPS xyplex:

   ```
   Trying...
   Connected to xyplex1.
   Escape character is '^]'.
   ```

b. Press the **Enter** key in order to get a **#** prompt from the AWIPS xyplex. At the #
    prompt, **enter the password access** followed by the **Enter** key (the access password
    will not be displayed as you type in the characters)

    #access

    After the access password is entered, the AWIPS xyplex will display the Following
    message:

    ```
    Welcome to AWIPS
    ```

c. Enter username>

    At the Enter username> prompt, enter the username **awips** followed by the Enter key:

    Enter username>**awips**

    After the awips username is entered, the AWIPS xyplex will display the Xyplex>
    prompt.

d. At the Xyplex> prompt, enter the command **c xyplex1:5800** command followed by a
    couple of **Enter** keys in order to get a login prompt from the Gauntlet Firewall server:

    Xyplex> **c xyplex1:5800**

    Following the c xyplex1:5800 command, the following messages appear:

    ```
    Xyplex -010- Session 1 to XYPLEX1:5800 established
    The Gauntlet(R) Internet Firewall V4.1 --  By Trusted
      Information Systems
    gw-gyx.wgyx.noaa.gov

    login:
    ```

e. At the Gauntlet **login** prompt, type **root** press **enter** then type in the **password** for
    the Gauntlet Firewall server.

3. As the **root** user on the Gauntlet Firewall server, use the **vi** editor to edit the
    /etc/ntp.conf file and add the following 3 lines where (see examples):
    ls1.ls1.ls1.ls1 is the IP address for the ls1 server (i.e, .140.92.18.127),
    dx1.dx1.dx1.dx1 is the IP address for the dx1 server (i.e., 165.92.18.3),
    dx2.dx2.dx2.dx2 is the IP address for the dx2 server (i.e., 165.92.18.4)

    broadcast ls1.ls1.ls1.ls1   Example: broadcast 140.92.18.127
    server dx1.dx1.dx1.dx1 prefer   Example: server 165.92.18.3 prefer
    server dx2.dx2.dx2.dx2   Example   server 165.92.18.4

    The 3 lines described in this step should be the only 3 lines in the /etc/ntp.conf file.

4. Stop and restart the xntpd daemon process running on the Gauntlet Firewall server.

   a. To get the process ID for the xntpd daemon process, enter the command:

      `ps -x | grep xntpd`

   b. Use the kill command to terminate the process ID associated with the xntpd process

   c. Restarted xntpd process by entering the command:

      `/usr/contrib/bin/xntpd`

5. End the root user session on the Gauntlet Firewall by entering the command `exit`. The exit command will return you to the login prompt for the Gauntlet Firewall. At the login prompt, close the telnet window.

   This completes the configuration for the Network Time Protocol on the Gauntlet Firewall server.

6. To verify that the AWIPS Gauntlet firewall is receiving the date/time information from the dx1/dx2 servers, you can monitor the `/usr/var/log/messages` file on the AWIPS Gauntlet firewall. Each day, the `/usr/var/log/messages` file should contain time synchronization messages such as the following:

   `Jan 20 14:26:15 gw-tae xntpd[107]: time reset (slew) -0.317355 s`